DITSCAP Primer

Center For Information Assurance Engineering (CFIAE)

DITSCAP* Authority

- **ASD/C3I Memo, 19 Aug 92**
  - **Develop Standardized C&A Process**
- **DODI 5200.40**
  - **Title: DoD Information Technology Security Certification and Accreditation Process (DITSCAP)**
  - **ASD Signature 30 Dec 97**
- **DOD 8510.1-M**
  - **Title: DITSCAP Application Manual**
  - **Standalone document supplementing DoDI 5200.40**
  - **ASD Signature 31 Jul 00**

SCAP: DoD Information Technology Security Certification and Accreditation Proc

DITSCAP Applicability*

- **Applies to**
  - **All DOD C/S/As**, Components, Activities, CJCS, and their Contractors and Agents**
- **Applies to**
  - **"the acquisition, operation and sustainment of any DoD system that collects, stores, transmits, or processes unclassified or classified information"**
  - **"Any IT or information system life cycle, …, the reconfiguration or upgrade of existing systems…"**
- **Effective immediately**
- **Mandatory for use by all DOD**

*** DODI 5200.40, 30 Dec 97, Para 2**
**** S/C/As: CINCs/Services/Agencies**

Why DITSCAP

DITSCAP

- **DoDI 5200.40 (DITSCAP) establishes a standard DOD-wide process, set of activities, general tasks, and a management structure to certify and accredit Information Systems (IS) that will maintain the Information Assurance (IA) and security posture of the Defense Information Infrastructure (DII) throughout the life cycle of the system**

Definitions

Certification

"Comprehensive evaluation of the technical and non-technical security features of an IT system and other safeguards, made in support of the accreditation process, to establish the extent that a particular design and implementation meets a set of specified security requirements"*

* DODI 5200.40, 30 Dec 97, Enclosure 2, para E2.1.8

Certification

Certification is a security analysis in the following areas:

- **Physical**
- **Personnel**
- **Administrative**
- **Information**
- **Information Systems**
- **Communications**

Definition

Accreditation

"Formal declaration by the DAA that an IT system is approved to operate in a particular security mode using a prescribed set of safeguards at an acceptable level of risk"*

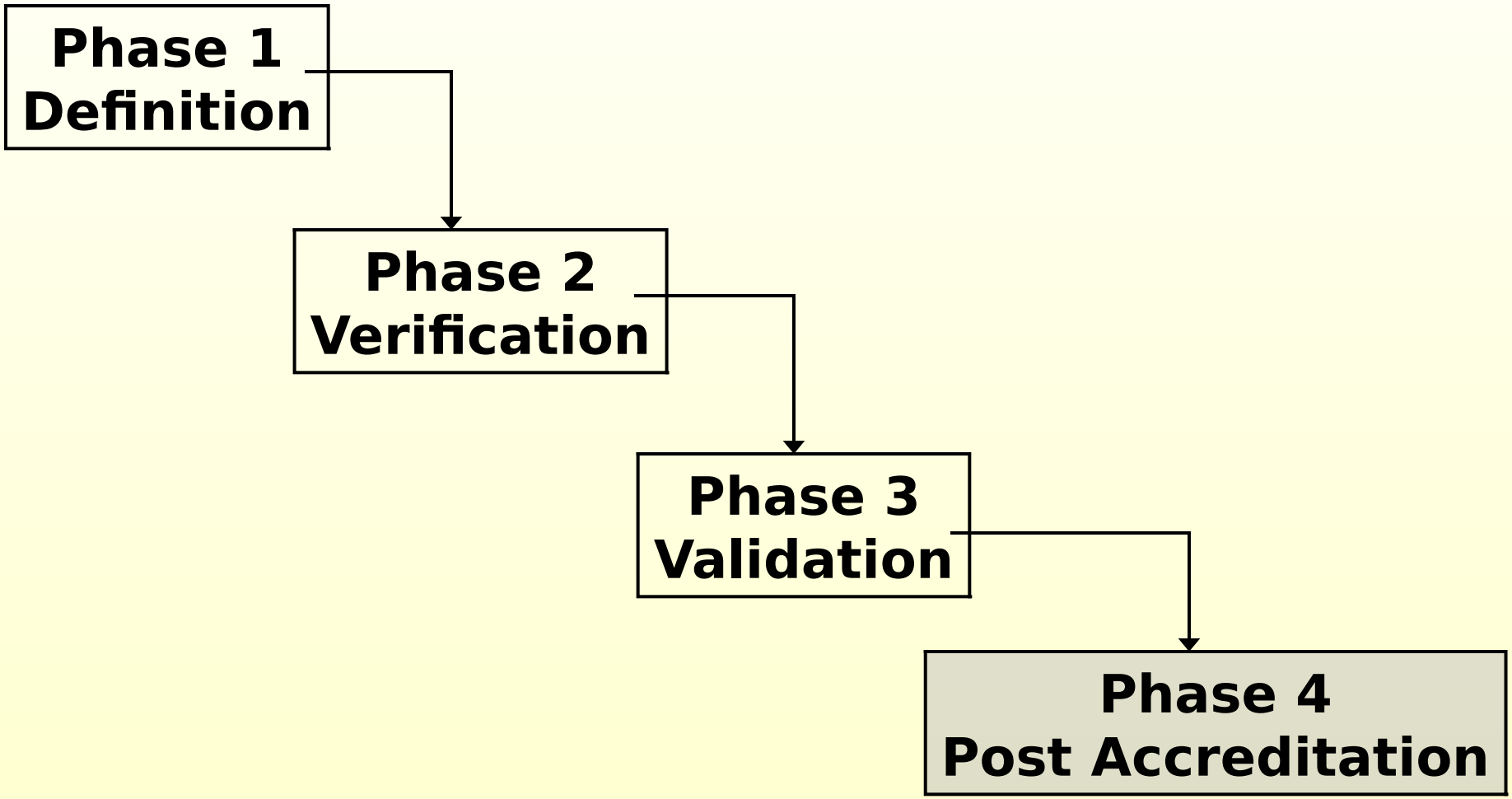
*** DODI 5200.40, 30 Dec 97, Enclosure 2, para E2.1.2**
DAA: Designated Approving Authority

DITSCAP Features

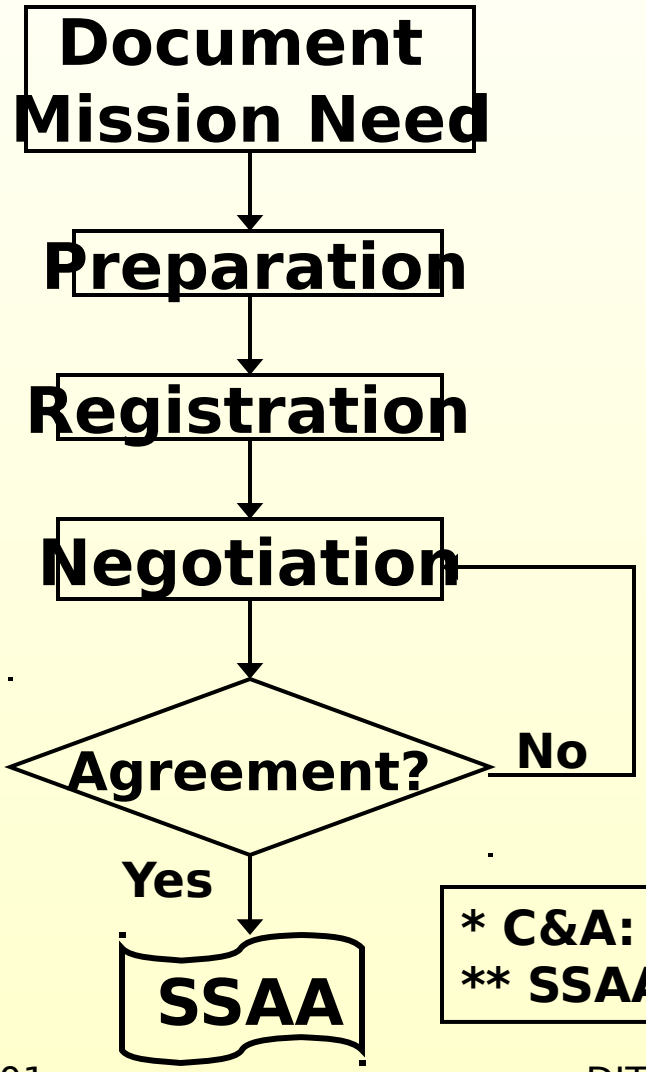
DITSCAP

- Defines a process for uniform C&A practice
- Applicable throughout life cycle of system
- Applicable to any type of acquisition strategy or development
- Should be part of the Acquisition Strategy
- Is a continuous process
- Brings responsible organizations together

DITSCAP Phases



Phase 1: Definition



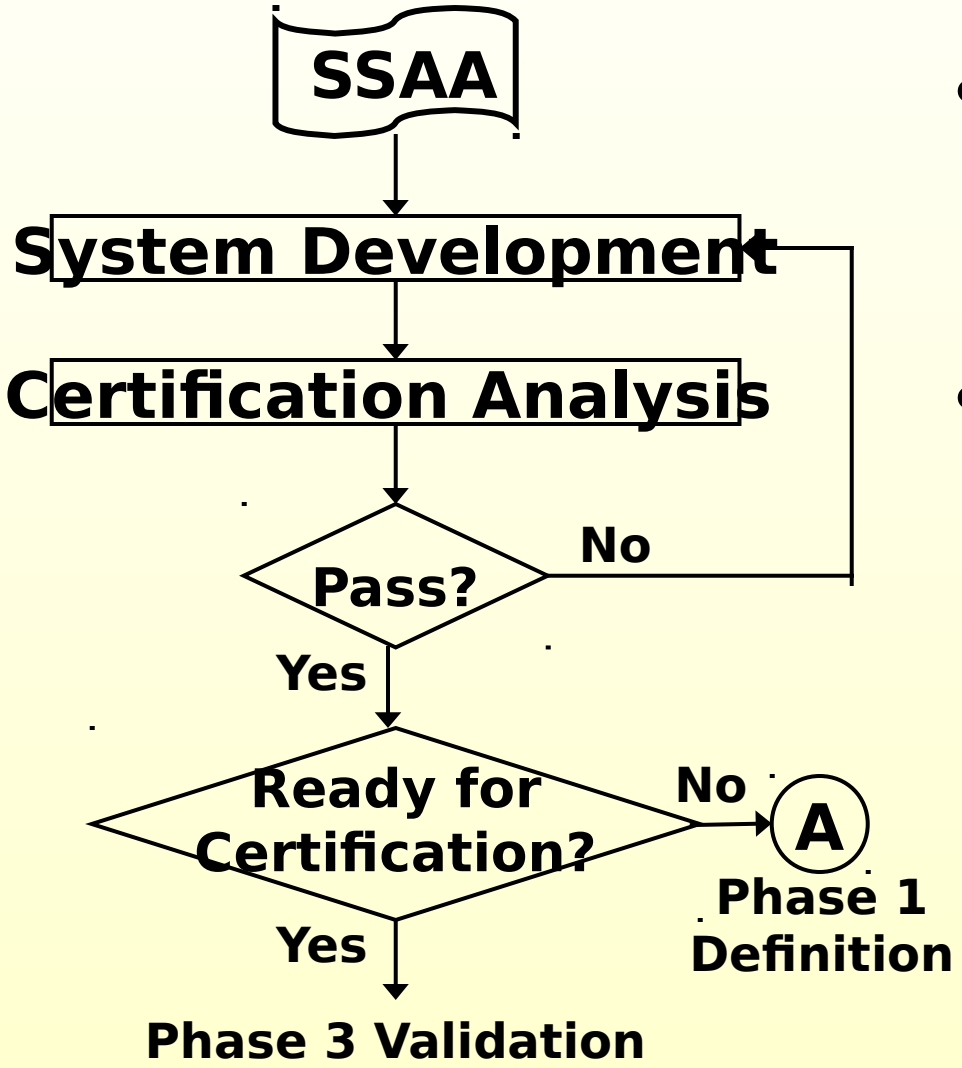
- Key players agree on the intended system mission, security reqs, C&A* boundary, schedule, level of effort, and required resources
- Agreement is documented in the SSAA**

* C&A: Certification and Accreditation
** SSAA: System Security Authorization Agreem

Phase 1 Main Tasks

- Define system functions, reqs, and interfaces
- Define information category and classification
- Prepare the system architecture description
- Identify principle C&A roles & responsibilities
- Define C&A level of effort
- Draft SSAA
- Agree on the method for implementing security reqs (documented in SSAA)

Phase 2: Verification

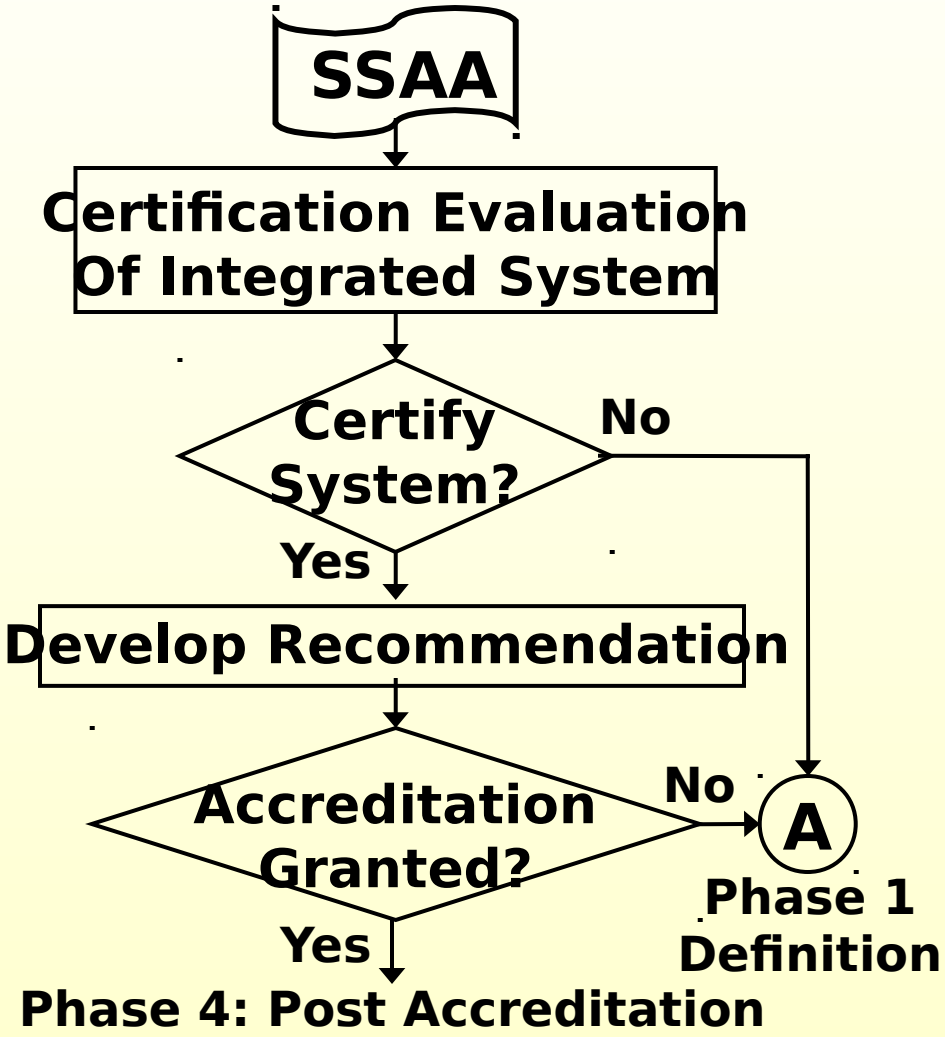


- Verify system's compliance with SSAA reqs
- Goal is to obtain integrated system for certification testing and accreditation

Phase 2 Main Tasks

- System Architecture Analysis
- Software Design Analysis
- Network Connection Rule Compliance
- Integrity Analysis of Integrated Products
- Life Cycle Management Analysis
- Security Reqs Validation Procedures
- Vulnerability Evaluation

Phase 3: Validation



- System on-hand
- Validates system compliance w/SSAA reqs
- Goal is to obtain full approval to operate system (accreditation)

Phase 3 Main Tasks

- **ST&E* (Implementation of security reqs, I&A, AC, Audits…)**
- **Penetration Testing (Exploitation, Insider/Outsider)**
- **COMSEC Compliance Evaluation (Reqs, Integration)**
- **System Management Analysis (Maintain Mgmt/CM/Arch)**
- **Contingency Plan Evaluation (Backup, COOP…)**
- **Site Accreditation Survey (SSAA compliance, environment)**
- **Risk Management Review (acceptable risks to CIAA**)**
- **Develop Certification Report and Recommendation for Accreditation:**
  - **System Certified: Yes or No (based on meeting SSAA reqs)**
  - **If Certified, Recommend: IATO or Accreditation**
- **Ends with accreditation decision from DAA**

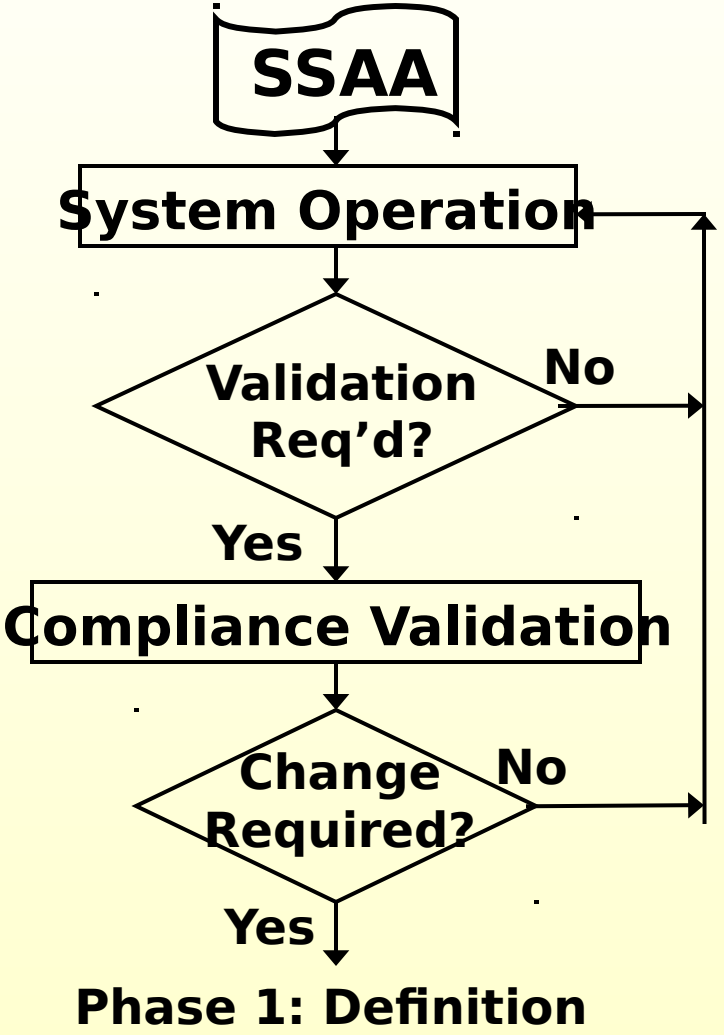
*** ST&E: Security Test and Evaluation**
**** CIAA: Confidentiality, Integrity, Availability, and Accountability**

ST&E Tasks*

- Assess implementation of security design
- Ascertain that CIAA are implemented as documented in SSAA and perform properly
- Validate correct implementation of I&A**, Audits, Access Controls, Object Reuse, Trusted Recovery, and Network Connection Rule Compliance
- Evaluate system conformance w/reqs, mission, and architecture as defined in SSAA

* DODI 5200.40, and DODM 8510.1
** I&A: Identification and Authentication

Phase 4: Post Accreditation



- Starts after site accreditation
- Objective is to maintain an acceptable level of residual risk
- DITSCAP responsibilities shift to site/O&M Orgs
- Ends with system termination

Phase 4 Main Tasks

- **Review configuration & security Mgmt***
  - **Follow change mgmt documented in SSAA**
  - **Determine if system security mgmt continues to support mission and architecture**
- **Conduct risk management review**
  - **Assess if risk to CIAA is being maintained at an acceptable level**
- **Conduct compliance validation if needed**
  - **Ensure continued compliance w/SSAA reqs, current threat assessment, and concept of operations**
- **Maintain SSAA**

*** Mgmt: Management**

Questions?

Answers:

- **IASE Web Site:**
  https://iase.disa.mil/ditscap/index.html
- **IASE Information Desk:**
  https://iase.disa.mil/IaseInfoDesk.html
- **E-Mail (unclassified): iase@ncr.disa.mil**
- **Phone: (703) 681-IASE (4273); DSN 761- 4273**